Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1705 01/30/15

~ Wikileaks Slams Google ~ Facebook Emoji Threats ~ The GHOST Bug!

-* Cuban Secret Computer Network *-
-* China Tightens Internet Control More *-
-* Facebook vs. 25,000 Users in Privacy Suit! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Well, it's been one helluva week as far as the weather was concerned! After about 6 inches of snow last weekend, here in New England, we got hit with another 2+ feet (yes, I said FEET) of snow earlier in the week! Fortunately, one way to consider it, it was light, fluffy snow that was easily cleared. What made things bad was the heavy winds that caused a lot of drifting; and, naturally, having the snow blow back in your face when trying to throw it somewhere.

Now we're all faced with trying to find a place to put all of this snow! Out here in the 'burbs, it's not too bad compared to those in the city. But, we're still faced with streets that weren't plowed completely, and sidewalks that haven't been cleared yet by the town. And, it can occasionally be difficult to see around corners because of the high piles of snow at intersections.

And to make matters even worse, the forecast for early next week is another foot of snow! I guess Mother Nature is trying to make up for the past couple of winters. Life in New England, I guess!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Reptile Returns in Mortal Kombat X
""""""""""""""""""""""""""""""""" Grim Fandango Remastered !

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Reptile Returns in Mortal Kombat X

Reptile, the acid spitting ninja that quickly won favor (or not thanks to his confusing invisibility ability in MK II), will be joining the lineup in Mortal Kombat X. This latest iteration of the Mortal Kombat series has been building anticipation thanks to a series of tantalizing reveals, new characters, and some of our favorite faces. It s about time too! Mortal Kombat fans (like yours truly) have been waiting since 2011 to get another taste of the funny and brutal combat that has made the series so unique. Want to see what kinds of carnage we can expect from Reptile in Mortal Kombat X? Check out the trailer below that includes some gameplay and even features Reptile executing one of his fatalities:

So who will Reptile be battling against in the forthcoming title? The roster currently features 13 characters (including Goro who s slated to be a pre-order exclusive only) and is a mix of new and familiar faces. The four new fighters who are waiting to spill blood (or spill theirs) are Kotal Kahn, Cassie Cage, D Vorah and the Ferra/Torr combination. Reptile will be reunited with some fan favorites that include Scorpion (obviously), Kitana, Raiden, and Kano. Reptile s inclusion in the exciting line up of kombatants isn t the only reason why Mortal Kombat fans are not so patiently waiting for Mortal Kombat X s April release. Each character will have multiple playable variants with each one getting its own distinctive look. Every character variant will feature unique combat abilities which means that to survive in Mortal Kombat X, you will need to use a completely different strategy.

With so many things to look forward to in the new Mortal Kombat X, it makes waiting for the April release all the more agonizing. PC, Xbox 360, Xbox One, PlayStation 3 and PlayStation 4 fans will be shouting Toasty! when its released on the aforementioned platforms on April 14th.

Grim Fandango Remastered Reanimates Some Really Funny Bones

One of the best games ever made about the afterlife has finally got one of its own.

After lying dormant for 17 years, Tim Schafer s seminal 1998 adventure game Grim Fandango has returned to the land of the living a place where its cast of skeletal rogues and ne er-do-wells would hardly feel at home.

The game s status as a masterpiece has been cemented by time. It s viewed as a pinnacle of the adventure genre, and it s one of the reasons we rated 1998 as the greatest year in video game history. But for a long time, it s been difficult to play the game on modern systems. That s no way to treat a classic: It s like if it were impossible to find a playable video recording of Rear Window or if The Great Gatsby had gone out of print.

The new Grim Fandango Remastered ($15 for PC, Mac, PS4, PS3, and PS Vita) redresses that injustice. It also presents two questions. First, how does it hold up? And second, are its extra goodies enough to justify a purchase for players who ve already clocked plenty of hours in the Department of Death?

As it turns out, Grim Fandango is still a good often great video game.

But the years have been kinder to its artistic components story, art direction, writing, audio than to its gameplay and interface.

For those who didn t catch this classic the first time around, Grim Fandango puts you in the shoes of Manny Calavera, a down-on-his-luck Grim Reaper/travel agent tasked with ushering newly departed souls to their destiny in the afterlife. When Manny falls in love with a beautiful client, he s drawn on an adventure that will take him from the offices of the Department of Death to the exotic port of Rubacava and beyond, encountering various lost souls and eccentric demons along the way.

The star of the show is the visual style, which mashes together all sorts of disparate elements Día de los Muertos costumery, art deco, Aztec sculpture, film noir, movies like Casablanca and Vertigo yet somehow keeps it coherent and unified. No game before or since has looked like Grim Fandango: It s absolutely unique. Allowing for the technical limitations of its time, it looks good enough to be a movie. This is Pixar-quality design in a 1998 adventure game package.

The writing and voice acting are first-rate, too. Tony Plana brings a resigned grace to the voice of Manny and is ably assisted by supporting players like Alan Blumenfeld (gigantic mechanic Glottis) and Patrick Dollaghan (Manny s annoyingly alpha co-worker Domino). The dialogue is sharp, clever, and breezy, winking at genre clichØs while moving the story along briskly.

Though the graphics have been tweaked a bit (Manny looks better, the backgrounds do not), the audio gets a much more thorough treatment, as the game s terrific score was rerecorded by a live orchestra.

Games aren t all sound and visuals, though. Grim Fandango belongs to a tradition of adventure game design that can be traced back through Schafer s equally loved Monkey Island games, Sierra s seminal King s Quest franchise, and even Infocom s text adventures of the early 1980s (think Zork). To say that these games are hard doesn t quite cut it. It s more that they re hard in arbitrary ways, requiring players to get in sync with the designer s twisted inner sense of logic.

Solving these puzzles is, as Salvador Dalí once said of painting, either easy or impossible. Forget the slow, methodical ratcheting up that teaches players the game mechanics. Grim Fandango is tough from the outset and periodically gets insane. Many players will be forced to consult a walk-through to complete some of the game s head scratchers, and that always leaves a bad taste.

The awkward interface doesn t help either. In a way, this 1998 game has a more primitive interface than its 1980s forebears. Playing Zork, I could type something like pick up the letter and put it on the table and the game would understand that. But with Grim Fandango, you have to figure out how to boil your actions down to an extremely simple vocabulary of click options that s mostly limited to use, pick up, and examine.

Because the game was made in an era before its lavish locations could be rendered in real-time 3D, all of the settings are static, viewable only from predetermined angles. This can make moving around disorienting, as the camera abruptly switches perspective (sometimes even within the same room, depending on your location). The camera choices seem to have been designed for visual impact more than for user convenience. And when you enter a new area, you ll likely fall into the habit of hovering your pointer around the screen until it changes, indicating something you can

interact with. That s playing the interface, not playing the game.

Still, flaws aside, the puzzle solutions (when reached honestly) impart a hefty dopamine drip, and you re tugged onward by a desire to see what new locations and characters the designers have in store. You find yourself drawn back to Grim Fandango even when you know it ll bring frustration.

The Remastered version delivers some nice extras, too. The director s commentary, featuring lead designer Schafer and several members of the game s original team, is full of interesting details about what inspired particular design choices in the game. It s also refreshingly not dumbed-down. These are professional game developers talking in their own lingo and not bothering to slow down to make sure you can keep up. For would-be game-makers and big fans of the game, it s a must-listen. There are also about a hundred pages of original concept art to flip through, though you ll need to complete the appropriate levels to unlock them.

Bottom line, it s a very good thing that Grim Fandango Remastered exists, and not only for the historical interest. If you can tolerate the interface annoyances and occasionally obtuse puzzles, it s unequivocally worth the $15 asking price, a singular experience that fans of adventure games shouldn t miss. Here s looking at you, Mr. Calavera.

What s hot: Unique; impeccable design, story, and voice acting; informative developer commentary
What s not: Clunky interface; arbitrary puzzle logic

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Super-cookie Crumbles: Verizon Will Kill Off Hated Zombie Stalkers

Verizon has backed down over its fingerprinting of subscribers using so-called immortal "super cookies."

In 2012, the US mobile telco started injecting unique identifying headers (UIDHs) into every HTTP request users made to websites via the Verizon network. This allowed sneaky ad agencies to recognize people as they moved from site to site, and display ads tailored to individuals’ interests.

Deleting all your cookies from your web browser, or using something like Chrome’s incognito mode, will not kill off the header because it is inserted automatically by the carrier.

Customers could "opt out" of the system, but the X-UIDH code would still be injected, allowing smart networks like Turn in San Francisco to follow people around the web regardless. The ad agency stopped doing that about a week ago.

The per-subscriber headers caused a stink among privacy warriors, due to the blanket nature of the injection and that it was impossible to remove it.
Campaigners at the EFF objected to the mandatory nature of the headers.

AT&T was testing a similar system, and dropped that when it was exposed.

Now Verizon has said that this time "opt-out" really means opt-out: it's going to stop injecting UIDHs into subscribers' web traffic if they switch off the system in their account settings.

Previously, if you opted out, stats about where you've been online were withheld from advertisers, but as we've seen with Turn, that didn't stop determined networks.

"Verizon takes customer privacy seriously and it is a central consideration as we develop new products and services. As the mobile advertising ecosystem evolves, and our advertising business grows, delivering solutions with best-in-class privacy protections remains our focus," the company told El Reg in a statement on Friday.

"We listen to our customers and provide them the ability to opt out of our advertising programs. We have begun working to expand the opt-out to include the identifier referred to as the UIDH, and expect that to be available soon. As a reminder, Verizon never shares customer information with third parties as part of our advertising programs."

Facebook vs 25,000 Users

An Austrian court has given the go ahead to a class action lawsuit brought against Facebook for alleged privacy violations across Europe.

Max Schrems' Europe v Facebook group, which originally filed the lawsuit in August 2014, has had an initial hearing date set for 9 April 2015, marking the first time that Facebook will appear in court over the complaint.

The class action asserts that Facebook violated users' privacy in a number of ways, including:

invalid privacy policies
the unauthorised use of data
supporting NSA spying via its PRISM surveillance program
tracking users on external websites via apps and its 'Like button'
unlawful introduction of 'Graph Search'
the passing on of user data to apps and third parties without authorisation
the use of 'big data' to analyse and monitor users' interactions

The purpose of the hearing will be to decide whether the social networking giant's objections to the admissibility of the case are valid.

According to a press release put out by Europe v Facebook, the company has claimed that "it cannot be sued" as the number of users bringing the action would be illegal in Ireland, home of its international HQ, because it would violate "public order."

Dr Proksch, lawyer for the plaintiffs, said:

We have reviewed all objections from Facebook in great detail and came to the conclusion that they lack any substance. It seems that they try to delay the procedure with partly really bizarre arguments.

The plaintiffs are demanding compensation of 500 ($565/£370) each in respect of the alleged privacy violations. The number of claimants has been capped at 25,000 for logistical reasons but it still represents "the largest privacy class action in Europe," according to Schrems.

A further 50,000 users have signed up to the class action via www.fbclaim.com and await news as to whether they will be allowed to join at a later date.

Beyond seeking a nominal level of damages, which would collectively amount to more than 10m, the group is also calling for a "suspension of data usage".

Europe v Facebook believes that Facebook’s business practices, which it describes as being "questionable," may be ruled illegal under Europe’s strict privacy laws.

China Further Tightens Control Over Internet

Jing Yuechen, the founder of an Internet start-up here in the Chinese capital, has no interest in overthrowing the Communist Party. But these days she finds herself cursing the nation s smothering cyberpolice as she tries and fails to browse photo-sharing websites like Flickr and struggles to stay in touch with the Facebook friends she has made during trips to France, India and Singapore.

Gmail has become almost impossible to use here, and in recent weeks the authorities have gummed up Astrill, the software Ms. Jing and countless others depended on to circumvent the Internet restrictions that Western security analysts refer to as the Great Firewall.

Lu Wei has ratcheted up China s sophisticated system of online censorship.

By interfering with Astrill and several other popular virtual private networks, or V.P.N.s, the government has complicated the lives of Chinese astronomers seeking the latest scientific data from abroad, graphic designers shopping for clip art on Shutterstock and students submitting online applications to American universities.

If it was legal to protest and throw rotten eggs on the street, I d definitely be up for that, Jing, 25, said.

China has long had some of the world s most onerous Internet restrictions. But until now, the authorities had effectively tolerated the proliferation of V.P.N.s as a lifeline for millions of people, from archaeologists to foreign investors, who rely heavily on less-fettered access to the Internet.

But earlier this week, after a number of V.P.N. companies, including

StrongVPN and Golden Frog, complained that the Chinese government had disrupted their services with unprecedented sophistication, a senior official for the first time acknowledged its hand in the attacks and implicitly promised more of the same.

The move to disable some of the most widely used V.P.N.s has provoked a torrent of outrage among video artists, entrepreneurs and professors who complain that in its quest for so-called cybersovereignty Beijing s euphemism for online filtering the Communist Party is stifling the innovation and productivity needed to revive the Chinese economy at a time of slowing growth.

 I need to stay tuned into the rest of the world, said Henry Yang, 25, the international news editor of a state-owned media company who uses Facebook to follow American broadcasters. I feel like we re like frogs being slowly boiled in a pot.

Multinational companies are also alarmed by the growing online constraints. Especially worrisome, they say, are new regulations that would force foreign technology and telecom companies to give the government back doors to their hardware and software and require them to store data within China.

Like their Chinese counterparts, Western business owners have been complaining about their inability to gain access to many Google services since the summer. A few weeks ago, China cut off the ability to receive Gmail on smartphones through third-party email services like Apple Mail or Microsoft Outlook.

The recent disabling of several widely used V.P.N.s has made it difficult for company employees to use collaborative programs like Google Docs, although some people have found workarounds for the time being.

 One unfortunate result of excessive control over email and Internet traffic is the slowing down of legitimate commerce, and that is not something in China s best interest, said James Zimmerman, chairman of the American Chamber of Commerce in China. In order to attract and promote world-class commercial enterprises, the government needs to encourage the use of the Internet as a crucial medium for the sharing of information and ideas to promote economic growth and development.

Chinese authorities have long had the ability to interfere with V.P.N.s, but their interest in disrupting such programs has mounted alongside the government s drive for cybersovereignty, especially since President Xi Jinping came to power two years ago. Lu Wei, the propaganda official Mr. Xi appointed as Internet czar, has been unapologetic in promoting the notion that China has the right to block a wide array of online content. A co-founder of Greatfire.org, which tracks online censorship in China, suggested the government had decided that soaring V.P.N. use among ordinary Chinese warranted a more aggressive attack on such software.

 This is just a further, logical step, said the co-founder, who requested anonymity to avoid government scrutiny. The authorities are hellbent on establishing ybersovereignty in China. If you look at what has taken place since last summer it is quite astounding. Government officials have denied any role in blocking Google and they have dismissed accusations that Chinese authorities were behind a man-in-the-middle attack on Outlook two weeks ago as well as other

hacking incidents involving Yahoo and Apple. But such claims have by and large fallen on deaf ears, especially given Beijing s strident campaign against the hostile foreign forces it says are seeking to undermine the country through the Internet. On Tuesday, however, a senior official at the Ministry of Industry and Information Technology acknowledged that the government was targeting V.P.N.s to foster the healthy development of the nation s Internet and he announced that such software was essentially illegal in China.

Cuban Youth Build Secret Computer Network Despite Wi-Fi Ban

Cut off from the Internet, young Cubans have quietly linked thousands of computers into a hidden network that stretches miles across Havana, letting them chat with friends, play games and download hit movies in a mini-replica of the online world that most can’t access.

Home Internet connections are banned for all but a handful of Cubans, and the government charges nearly a quarter of a month’s salary for an hour online in government-run hotels and Internet centers. As a result, most people on the island live offline, complaining about their lack of access to information and contact with friends and family abroad.

A small minority have covertly engineered a partial solution by pooling funds to create a private network of more than 9,000 computers with small, inexpensive but powerful hidden Wi-Fi antennas and Ethernet cables strung over streets and rooftops spanning the entire city. Disconnected from the real Internet, the network is limited, local and built with equipment commercially available around the world, with no help from any outside government, organizers say.

Hundreds are online at any moment pretending to be orcs or U.S. soldiers in multiplayer online games such as "World of Warcraft" or "Call of Duty." They trade jokes and photos in chat rooms and organize real-world events like house parties or trips to the beach.

"We really need Internet because there’s so much information online, but at least this satisfies you a little bit because you feel like, ’I’m connected with a bunch of people, talking to them, sharing files," said Rafael Antonio Broche Moreno, a 22-year-old electrical engineer who helped build the network known as SNet, short for streetnet.

Cuba’s status as one of the world’s least-wired countries is central to the new relationship Washington is trying to forge with Havana. As part of a new policy seeking broader engagement, the Obama administration hopes that encouraging wider U.S. technology sales to the island will widen Internet access and help increase Cubans’ independence from the state and lay the groundwork for political reform.

Cuban officials say Internet access is limited largely because the U.S. trade embargo has prevented advanced U.S. technology from reaching Cuba and starved the government of the cash it needs to buy equipment from other nations. But the government says that while it is open to buying telecommunications equipment from the U.S., it sees no possibility of changing its broader system in exchange for normal relations with the U.S.

Outside observers and many Cubans blame the lack of Internet on the

government’s desire to control the populace and to use disproportionately high cellphone and Internet charges as a source of cash for other government agencies.

Cuba prohibits the use of Wi-Fi equipment without a license from the Ministry of Communications, making SNet technically illegal. Broche Moreno said he believes the law gives authorities latitude to allow networks like SNet to operate. He described a sort of tacit understanding with officials that lets SNet run unmolested as long as it respects Cuban law its hundreds of nodes are informally monitored by volunteer administrators who make sure users don’t share pornography, discuss politics or link SNet to illicit connections to the real Internet.

"We aren’t anonymous because the country has to know that this type of network exists. They have to protect the country and they know that 9,000 users can be put to any purpose," he said. "We don’t mess with anybody. All we want to do is play games, share healthy ideas. We don’t try to influence the government or what’s happening in Cuba ... We do the right thing and they let us keep at it."

Users who break rules can be blocked from the network by their peers for as a little as a day for minor infractions such as slowing down SNet with file-sharing outside prescribed hours, with lifetime bans for violations like distributing pornography.

"Users show a lot of respect for preserving the network, because it’s the only one they have," Broche Moreno said. "But me and the other administrators are watching things to make sure the network does what it’s meant for."

The Cuban government did not respond to a request for comment on the network.

Before Obama moved to restore full diplomatic ties with Cuba, the U.S. made several attempts to leverage technology against the Cuban government. Contractor Alan Gross was sentenced to 15 years in prison after a U.S. Agency for International Development contractor sent him to Cuba to set up satellite Internet connections. He was freed after five years as part of the deal last month that paved the way for Obama’s new Cuba policy.

A separate USAID contractor tried to build a text message-based social network called Zunzuneo whose brief existence was revealed in an Associated Press investigation last year.

Joining SNet requires resources out of reach of many people in a country where the average salary hovers around $25 a month.

Humberto Vinas, 25, studied medical technology and accounting before finding a relatively well-paying job in the kitchen of a bar. He and nine friends shared an SNet node for several months, running hundreds of feet of Ethernet cable over neighbors’ roofs until one demanded they take it down, disconnecting most from the network.

"I miss SNet a lot," he said sadly. "You can find out about soccer scores. It allows you to do so much, right from your home."

Cubans have one of the hemisphere’s highest average levels of education and years of practice at improvising solutions to scarcity, allowing many to access and share information despite enormous barriers. For as little

as a dollar a week or less, many Cubans receive what’s known as "the package," weekly deliveries of pirated TV shows, movies, magazines and instructional texts and videos saved on USB memory drives.

There is no obvious indication the U.S. or any other foreign government or group had anything to do with the creation of SNet, making it by far the most impressive example of Cuba’s homemade telecommunications engineering.

The network is a series of connected nodes, powerful home computers with extra-strong Wi-Fi antennas that communicate with each other across relatively long distances and distribute signals to a smaller network of perhaps a dozen other computers in the immediate vicinity.

SNet started as a handful of connected users around 2001 and stayed that way for a decade. More than 9,000 computers have connected over the past five years, and about 2,000 users connect on an average day.

Many use SNet to get access to popular TV shows and movies. The system also stores a copy of Wikipedia. It’s not necessarily current, but is routinely refreshed by users with true Internet access. There’s also a homegrown version of a social network that functions similarly to Facebook.

Because most data passes from computer to computer in SNet, everything takes place much faster than on the achingly slow and expensive connections available from government servers that pass all information through central points.

Broche Moreno estimated it costs about $200 to equip a group of computers with the antennas and cables needed to become a new node, meaning the cost of networking all the computers in SNet could be as little as $200,000. Similar but smaller networks exist in other Cuban cities and provinces.

"It’s proof that it can be done," said Alien Garcia, a 30-year-old systems engineer who publishes a magazine on information technology that’s distributed by email and storage devices. "If I as a private citizen can put up a network with far less income than a government, a country should be able to do it, too, no?"

Teen Arrested After Alleged Facebook Emoji Threats

Emojis are words too.

Indeed, some might see them as a very modern, exalted form of digital cursive script.

That seems to be the view of the New York Police Department, after it viewed the Facebook page of 17-year-old Osiris Aristy from Bushwick, Brooklyn.

Aristy posted images of himself with guns and words such as: feel like katxhin a body right now.

However, as DNAInfo reports, he also posted images of little gun emojis pointing at little emoji heads of police officers.

Despite his young age, Aristy apparently has something of a police record, with 12 arrests, according to DNAInfo, for alleged offenses including criminal possession of a weapon, robbery and assault.

His Facebook page was, it seems, part of routine police surveillance. When the emojis and other messages were spotted, Aristy became an arrestee. And among the charges is making terrorist threats, according to DNAInfo. The publication goes on to say that the criminal complaint offers this: As a result of this conduct, the defendant has caused the informant and other New York City police officers to fear for their safety, for public safety, and to suffer alarm and annoyance.

Inspector Maximo Tolentino of the 83rd Precinct told DNAInfo: You make a threat on the internet, we re going to be watching.

I have contacted the 83rd Precinct seeking comment and will update, should I hear.

CBS New York reported that one of the offending posts read: N**** run up on me, he gunna get blown down. This was accompanied by the emoji of a police officer s head and then three enojis of a gun pointing in the head s direction.

The police also told CBS New York that Aristy had posted a selfie with his gun in the waistband of his pants. The New York Post said that Aristy had used Facebook to brag about owning a .38 gun.

There s surely an ever heightened awareness of social media threats to the police after the heinous murder of two officers in New York last month. The alleged culprit had previously made threats to the police on his Instagram account.

Aristy s lawyer, Fred Pratt, insists that his client meant no harm. He told DNAInfo: I understand that people found what he said distasteful and uncomfortable, but he never threatened to take action against police.

How can the police or anyone tell whether a social media threat is real or not? So many people use social media to vent, rant and generally attempt to impress anyone who might be bothered to listen.

How much time must officers now spend scouring the ill-thought-out (or not) postings of suspicious (or not) individuals in order to identify real threats?
Pratt s lawyer is using this very argument: How can the police tell?

With the hundreds of millions now posting to Facebook and many other sites, there s an infinity of possibilities, an infinity of potential danger.

Every word, every picture and, indeed, every emoji could mean something. Or it could mean nothing at all.

WikiLeaks Slams Google for Handing Over Emails to U.S. Government

Whistleblowing site WikiLeaks on Monday accused Google of handing over the emails and electronic data of its senior staff to the US authorities

without providing notification until almost three years later.

Google was apparently acting in response to warrants issued by the US Department of Justice, which is investigating WikiLeaks for publishing hundreds of thousands of classified military and diplomatic files.

WikiLeaks said the allegations against it point to a far broader investigation into its activities than the US authorities have previously indicated.

Alleged offenses range from espionage to theft of US government property and computer fraud and abuse, it said.

"Today, WikiLeaks lawyers have written to Google and the US Department of Justice concerning a serious violation of the privacy and journalistic rights of WikiLeaks staff," the site said in a statement.

WikiLeaks said that Google could and should have resisted complying with the warrants, as well as immediately informing those whose data it handed over.

The warrants demanded emails, contacts and IP addresses relating to the Google accounts of investigations editor Sarah Harrison, section editor Joseph Farrell and spokesman Kristinn Hrafnsson.

"We want to know why the three journalists were not notified of being spied (upon)," Harrison said at a press conference in Geneva.

Baltasar Garzon, a former Spanish judge who is Assange s lawyer, told reporters at the event: We believe the way the documents were taken is illegal .

He said that a law restricted for national security was used against their privacy and he threatened legal action against Google and US authorities.

The information was handed over to the US authorities on April 5, 2012, but Google did not inform the WikiLeaks staff until December 23, 2014, according to documents obtained by AFP.

"While WikiLeaks journalists, perhaps uniquely, do not use Google services for internal communications or for communicating with sources, the search warrants nonetheless represent a substantial invasion of their personal privacy and freedom," the organisation added.

WikiLeaks has been targeted by the US authorities since its release in 2010 of 500,000 secret military files on the wars in Afghanistan and Iraq and 250,000 diplomatic cables.

A former army intelligence analyst, Chelsea Manning, is currently serving a 35-year prison term for leaking classified documents to WikiLeaks.

WikiLeaks founder Julian Assange also believes he is a target for prosecution and has been holed up at the Ecuadoran embassy in London since 2012.

He sought asylum there to avoid being sent to Sweden, where he faces allegations of rape and sexual molestation which he denies. He says his extradition to Sweden could see him transferred on to the United States.

"His conditions are worse than all other detainees since he can not go outside, have a little walk in the garden for instance, without being arrested," his lawyer Garzon said on Monday.

In a statement to AFP, Google said it did not comment on individual cases, but said: Obviously, we follow the law like any other company.

"When we receive a subpoena or court order, we check to see if it meets both the letter and the spirit of the law before complying.

"And if it doesn t we can object or ask that the request is narrowed. We have a track record of advocating on behalf of our users."

It is not the first time WikiLeaks has clashed with the online giant.

In September 2014, Assange published a book, When Google Met WikiLeaks , questioning the Internet firm s close ties with the US administration.

FTC to Internet of Stuff: Security, Motherf****r, Do You Speak It?

US regulator the FTC says now is not the time for new laws on the "Internet of Things" but security needs to be improved as we enter the era of always-on, always-connected gadgets, sensors and machines embedded in homes, streets and pockets.

In a report [PDF] published today, the commission’s staff make a number of policy recommendations for the wave of new devices that collect and transmit data on our everyday lives.

From the camera that posts pictures online with a click, to automated home lighting and heating, to FitBits and Apple Watches, the Internet of Things (IoT) was the focus of this year’s Consumer Electronic Show, as well as a speech by FTC chairwoman Edith Ramirez.

There will be 25 billion devices connected to the internet by the end of the year, doubling to 50 billion by 2020, according to Cisco’s estimates. The problem is that many of the companies churning out these gizmos are not properly considering the risks associated with gathering masses of personal sensitive data, we’re told.

Security, and ultimately the safeguarding of privacy, is the biggest problem, says the FTC. And it needs to be built "into devices at the outset rather than as an afterthought." Employees also need to be trained up on the importance of security so there is a company-wide understanding and approach to protecting data, both internally and with any third parties that companies work with.

Additional measures such as good network defenses to prevent unauthorized users from getting access to data, and keeping an eye on security holes and providing security patches on time, should also be key considerations.

Given that, for example, home router makers are so slow to patch security vulnerabilities in firmware, what luck does anyone have fixing critical flaws in their IoT light switches, boilers and shoes?

As well as security, companies jumping on the IoT bandwagon should also think about "data minimization", meaning limit the amount of information

that is gathered and only retain it for a certain period of time.

The FTC's logic of that approach is that the fewer sensitive bytes companies hold, the less of a target their database will be (in theory) and the less opportunity exists for it to be used in ways that customers would be unhappy about.

Alternatively, companies could go out of their way to "de-indentify" data so it cannot be linked to specific individuals.

What you got?

In a related point, the FTC recommends that businesses adopt a "notice and choice" approach to data, ie: customers are informed what records the company gathers and are given the choice to opt out of its collection.

In order to prevent people from being overwhelmed with approval requests, the commission recommends that this "notice and choice" approach is adopted for any uses that would be "unexpected", ie: not immediately obvious to the consumer.

Obviously, this is something for lawyers to have fun with: sadly, is a photo-sharing app monitoring your movements really "unexpected" in this day and age?

If companies immediately de-identify data erase any way to pick out a particular person from the information the need to offer choices is greatly reduced, apparently.

As for legislation, the FTC report acknowledges that new laws may be needed at some point, but that it is too early to do so "given the rapidly evolving nature of the technology." As such, it sees self-regulation as the best way forward.

It does note however that the commission called for broad privacy legislation back in 2012, including breach notification laws, and that remains its position.

It is worth noting that the report was published only after four of the five commissioners voted in favor of doing so. The fifth commissioner, Joshua D Wright, published a dissenting opinion [PDF] and argued that the document is a weird hybrid between a writeup of discussions and a formal policy statement.

He would prefer one or the other, not a seemingly rushed mix of the two.

The report itself was based on a workshop held back in November 2013, and referred to subsequent public comments on the session. But the report as presented includes a range of policy recommendations.

Wright argues that if the FTC's staff wishes to produce policy recommendations, it needs to back them up with data, rather than "merely rely upon its own assertions." A workshop report should be a report of what people said; a formal report should "possess and present evidence that its policy recommendations are more likely to foster competition and innovation than to stifle it," he argues.

Hotels That Block Personal Wi-Fi Hotspots Will Get Busted, Says FCC

The US Federal Communications Commission (FCC) didn’t mince its words: hotels that block Wi-Fi are breaking the law.

From a warning posted on Tuesday:

In the 21st Century, Wi-Fi represents an essential on-ramp to the internet. Personal Wi-Fi networks, or "hotspots", are an important way that consumers connect to the internet. Willful or malicious interference with Wi-Fi hotspots is illegal.

In fact, blocking of guests’ personal hotspots violates Section 333 of the Communications Act, according to the FCC.

In spite of the illegality of such blocking, the Commission’s Enforcement Bureau has seen a "disturbing trend" in which hotels and other commercial establishments block wireless consumers from using personal Wi-Fi hotspots on their premises.

The Bureau has been investigating and taking action against Wi-Fi blocking, most notably with Marriott International Inc.

The hotel chain was investigated in 2014 and then slapped with a $600,000 fine (around £400,000).

But that didn’t stop it from waging a legal and PR battle to get permission to block personal hotspots in its conference and convention areas.

Earlier this month, Marriott threw in the towel on the blocking, though it said it hadn’t given up trying to get the FCC’s blessing on blocking in cases of "clear cybersecurity risk".

In spite of Marriott’s claims about cybersecurity, the FCC said on Tuesday that the hotel chain had admitted that blocked customers hadn’t posed a security threat to its network.

The "we’re doing it for their own good" argument was hard to swallow, in light of how much Marriott was making from selling internet "on-ramps" to the guests whose internet tires it had slashed: namely, between $250 to $1,000 per device to get onto the internet at one of its properties, according to the Commission.

Or, in the words of one reader,

Security my a**.....

The FCC says it will "aggressively" investigate and act upon "unlawful intentional interference".

Stay tuned: it says its Enforcement Bureau is investigating several complaints.

Hotels, a word to the wise: stop blocking the on-ramps, lest the FCC steamroll you.

US Military Wants To Replace Passwords With "Cognitive Fingerprints"

Researchers at the US military's elite West Point military academy have been awarded a multi-million dollar contract to produce a new identity verification system based on users' behaviour.

The technology, described as 'a next generation biometric capability', is being developed as part the active authentication programme run by DARPA (the Defence Advanced Research Projects Agency).

Authentication has traditionally relied on users producing one or more of the following: something you know (such as a passwords or PIN), something you have (such as a number from an RSA key) or something you are (such as your fingerprints or face.)

The technology that West Point is working on, behaviour-based biometrics, adds another factor to the mix: something you do.

According to DARPA the first phase of the active authentication program will focus on biometrics that can be captured through existing technology, such as analysing how the user handles a mouse or how they craft the language in an email or document.

The contract document, seen by Sky News and reported by Yahoo Finance, describes the technology as a "cognitive fingerprint":

...when you interact with technology you do so in a pattern based on how your mind processes information, leaving behind a 'cognitive fingerprint'

The biometrics program is creating a next generation biometric capability built from multiple stylometric/behavioural modalities using standard Department of Defence computer hardware.

If they're effective, cognitive fingerprints could offer significant advantages over existing forms of authentication.

Unlike biometrics they don't require specialist hardware and unlike password authentication they doen't rely on users being good at something they're naturally bad at.

The technology should also give systems the ability to authenticate users continuously, keeping people logged in so long as they're present and then logging them out as soon as they leave.

The need to replace passwords in particular is pressing.

Generating and remembering effective passwords is difficult and unnatural. A lot of us are awful at it and there's almost no improvement in the list of most common passwords from year to year. Meanwhile, computers improve their ability to crack passwords by brute force and cunning every year.

Biometrics has been waiting in the wings as the Next Big Thing in authentication for years.

While biometrics are used in household and business products, as a family of technologies it hasn't come close to supplanting passwords.

Transparent, behaviour-based biometrics could provide the nudge that's needed to push biometrics into the mainstream, but there are two major obstacles to overcome before that happens.

The first is that you can’t change your biometrics - so what’s the equivalent of changing your password if you’re compromised?

The second is that for all the frustration that comes with remembering (and forgetting) our passwords, we know and feel, tangibly, that they’re under our control.

Behaviour-based biometrics will happen invisibly, which will be convenient but it will require us to be comfortable ceding that feeling of control too.

Precursors to behaviour-based biometrics - technologies that determine things about us based on the way we behave - are already with us.

In December 2014, Google completely reinvented it’s reCAPTCHA product, replacing the annoyingly wibbly wobbly letters and the out of focus photos with a simple tick box.

The tick box, backed by Google’s trove of user data and a hat full of artificial intelligence, determines if you’re a human based on what it knows about you and how you tick the box.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) are tests used to tell whether an action performed is carried out by a human or a computer (normally so that the activity of computers can be ignored.)

Over time computers have got better at solving CAPTCHA puzzles, forcing us real humans to contend with increasingly frustrating and difficult to disentangle puzzles.

What Google realised was that advances in Artificial Intelligence that make it easier for unfriendly computers to guess "what number is in this photo?" also make it easier for friendly computers to solve difficult puzzles like "is this computer user behaving like a computer or a human?"

I think the Google reCAPTCHA change gives a hint at just how dramatic a shift to behaviour-based biometrics could be for both security and user experience.

We’d better get used to our new robot overlords.

The GHOST Vulnerability - What You Need To Know

The funkily-named bug of the week is GHOST.

Its official moniker is the less catchy CVE-2015-0235, and it’s a vulnerability caused by a buffer overflow in a system library that is used in many, if not most, Linux distributions.

A buffer overflow is where you assume, for example, that when you handle a four-byte network number written out as decimal digits, you will never get anything longer than 255. 255. 255. 255.

That takes up 15 characters, so you may decide that you’ll never need more than 15 bytes of memory.

So, if you add a spare byte for luck and allocate 16 bytes, you're bound to have enough space.

And then, one day, a malicious user decides to see what happens if he ignores the rules, and uses a network number like, say, 1024. 10224. 102224. 1022224.

That network number is nonsense, of course, but your program might not hold out long enough to reject it.

Your code will probably crash right away, because the attacker's 25 bytes will overflow your 16 bytes of available memory.

As it happens, the GHOST vulnerability is connected with network names and numbers.

The spooky name comes from the system functions where the vulnerable code was found.

The functions are called gethostby›name() and gethostby›name2(), and they do what the names suggest.

They find the computer-friendly network number of a host (e.g. 93. 184. 216. 34) from its human-friendly name (e.g. example.com).

In other words, these functions do a DNS (domain name system) lookup for you, so your program doesn't need to deal with the intricacies of the DNS protocol.

By the way, even if your program doesn't directly call gethostby›name(), you may end up calling it indirectly as a side-effect of doing something, anything, involving a computer name.

For example, if your software looks up email addresses, calls home for updates, retrieves postings from online forums, plays podcasts, or any of a number of perfectly unexceptionable network-related activities, it almost certainly triggers name-to-number lookups at some point.

And if those lookups are based on data received from outside, such as a sender's email address in received email headers, then attackers may very well get to choose what data gets passed to your Linux computer's gethostby›name() function.

It turns out that gethostby›name() has a clever feature, where it works out whether you called it with name that is already a network number (digits-dot-digits-dot-digits-dot-digits).

In that case, it would be a waste of time to do a DNS lookup, so it doesn't bother.

Unfortunately, the code that runs through the name to see if it's really a network number has a buffer overflow, and if you deliberately send a super-long number laid out just right...

...poof the GHOST strikes!

So an attacker may be able to rig up messages or network requests that crash your program; and with a bit (or, more likely, a lot) of trial and error, they might be able to trigger that crash in a way that gives them

control over your computer.

That’s known as a Remote Code Execution (RCE) exploit, similar to the bug recently found in the super-secure Blackphone, though in that case it was a text message that caused the phone’s software to trip over itself.

The good news is that this bug doesn’t exist on every computer.

It actually exists only in some versions of a software module called glibc, short for GNU C library.

In fact, most computers in the world don’t have glibc installed, because it’s not used by default on Windows, OS X, iOS or Android.

The bad news is that many, if not most, computers running Linux do use glibc, and may be at risk.

In short, therefore, if you have any Linux-based systems, including home firewalls and routers:

Check with your vendor, or the maker of your distribution, to see if you need a patch.

If you do, make plans to apply the patch as soon as you can.

Oh, and if you are a programmer, you shouldn’t really be using the gethostby›name functions anyway.

They were superseded many years ago by the much more flexible and useful function getaddr›info(), which you should use instead.

Facebook: Oi, Lizard Squad We Can Take Down Our Own Site, Ta

A technical cockup rather than hostile hacker action is apparently the reason Facebook, Instagram and other Web 2.0 sweethearts fell off the internet on Monday.

Prankster hacking crew Lizard Squad was gloating over the downtime; Tinder also disappeared for a while during the outage of Facebook and its photo-sharing sister site Instagram.

Security experts were unconvinced it was caused by a distributed denial-of-service assault. Facebook also dismissed any suggestion it was DDoSed; its techies blame technical problem for the hour-long outage:

Facebook and Instagram experienced a major outage tonight from 22:10 until 23:10 PST. Our engineers identified the cause of the outage and recovered the site quickly.

You should now see decreasing error rates while our systems stabilize. We don’t expect any other break in service. I’ll post another update within 30 mins. Thank you for your patience.

It’s understood a dodgy configuration change was pushed to Facebook’s API servers, which caused them to fall over.

Hipchat blamed "database issues", while Tinder joked by making a reference

to snow storms ravaging the north-eastern United States, and the recent Sony megahack. "EVERYBODY PANIC! ?#Blizzard?? North Korea? ?#TindernetApocalypse?," it said on Twitter.

Staffers behind AOL Instant Messenger (AIM) service are yet to comment on the incident. A trusted El Reg contact told us MySpace wasn't down, as Lizard Squad claimed, which suggests it was nothing but a dig by the miscreants at the unfashionable service.

The mass outage incident, which is rare but not unprecedented, illustrates the brittleness of social media services. A haiku El Reg's back-bench staff put together to mark a previous ?#facebookdown? day last June can be found here.

Security expert Professor Alan Woodward of the University of Surrey said that Lizard Squad's boasts underline how easy it is for jokers to get publicity through unsubstantiated claims.

"The recent outage of Facebook and the subsequent speculation that it may be a cyber-attack demonstrates the difficulty in reporting cyber-attacks," Professor Woodward said. "Facebook has confirmed that the downtime was caused by an engineering mistake.

"However, the Lizard Squad had only to mention the problem on Twitter and it caused instant speculation that it was they who had caused the problem. In the same way that it is very difficult for law enforcement agencies to attribute blame for cyber-attacks, it is very easy for hacking groups to plausibly claim any significant online incident as their work," he added.

Lizard Squad is best known for launching the denial of service attacks that took down the XBox Live and PlayStation Networks at Christmas, shortly before launching a DDoS-for-hire service.

Over the weekend it ran a DNS redirection attack that hijacked surfers trying to reach the website of Malaysia Airlines and presented them with a defacement page instead.

The hacktivists claimed they hacked the main servers, swiping corporate emails and other sensitive information in the process. However, as with the latest attack there is nothing to substantiate this claim.

When Facebook's Down, Thousands Slow Down

An outage that took Facebook and Instagram off the air for an hour Monday affected 29 locations where Facebook operates servers. Curiously, its massive Prineville, Ore., data center complex appears to have remained in operation throughout the outage.

That means a problem arose in the content distributing sub-data centers that Facebook has scattered around the US and around the globe, in both its own and colocation data centers. A map produced by an Internet metrics collecting firm, Dynatrace, indicates 29 such locations had their operations interrupted for an hour, starting about 9:10 p.m. Pacific time.

As a result, at least 7,500 Web sites that depend on a JavaScript response from a Facebook server had their operations slowed or stalled by a lack of

response from Facebook. Of course Facebook users, who could access the service, couldn’t get it to respond or do anything for them during the hour.

That’s just one of the conclusions an observer can make after examining data from Dynatrace, which tracks website performance for major retailers, financial services ecommerce systems, and online operations for hundreds of enterprises.

Dynatrace has 100 computers around the globe collecting data from "tens of thousands" of headless users, real-world end-users who allow their computers to periodically fire off stored queries to Nike, Netflix, and thousands of other online destinations. The client machines capture the response time and report it to Dynatrace. That allows it to report on application performance to their customers, which include Wells Fargo, LinkedIn, Cisco, Thomson Reuters, and Intuit.

Another conclusion is that the outage was not caused by a cyberattack, even though a group that wanted to claim credit started issued tweets claiming responsibility. Instead, Facebook ’fessed up to a configuration change gone awry.

"This was not the result of a third-party attack but instead occurred after we introduced a change that affected our configuration systems," according to Facebook’s statement.

From its position astride the Internet, Dynatrace said the slowdown of sites that use the familiar Facebook link "Like this page," or are otherwise dependent on Facebook interactions, illustrates the vulnerability of businesses that rely on third-party links to their websites.

Vincent Geffray, a senior product manager at Dynatrace, said its Outage Analyzer service is a big data application sitting on top of the data routinely captured by its application performance management monitoring. Outage Analyzer spotted a slowdown Monday that was simultaneously occurring at the websites of Dynatrace customers and traced it back to their ties to Facebook. In some cases, a site allows a visitor to log in using his Facebook identity. In others it responds to a "like" recorded on the Dynatrace customer’s site.

Dynatrace has 5,800 customers around the globe. Geffray said the Facebook slowdown occurred simultaneously around the globe. That suggests that the Facebook configuration change, the cited cause, may have been attempted to be implemented rapidly at several sites, spreading to other sites, or even implemented globally at the same time. The Dynatrace monitoring shows a sharp spike.

"We’re working to get things back to normal as quickly as possible," Facebook spokeswoman Charlene Chian told CNN. Facebook visitors were not totally cut off from their favorite social media. "Sorry, something went wrong," they were told as they tried to access the site.

For retail and enterprise sites that use Facebook as a third-party service, however, the incident took on serious consequences. According to Dynatrace, the short delays that started to show up around 9:10 p.m. PT grew into 39-second delays before a "server not available" or other message was returned to users. The retailers and other businesses were available, but their full pages couldn’t move to the next user interaction until the Facebook link finished loading its JavaScript.

In some cases, the inability of the end user’s computer to finish building a full page meant that his or her interaction with a target site would be very slow or stall completely.

"Let’s say Nike is slow because of Facebook. The customer doesn’t know that the degradation is due to Facebook. He just says, ’Nike is slow,’" Geffray said.

The problem exists with any social media service or other third party tied into a website’s operation. If the full document object model called for by the download can’t be built, due to absent JavaScript, the download may fail. Most websites are built with such interdependencies today. Their owners aren’t always aware of the ways a third party might be slowing down the site.

Whatever the cause, Facebook rectified the issue within the hour, and sites began to recover normal operations. Facebook has had a strong reliability record on the whole. Its last major outage was five years ago and lasted for 2.5 hours.

Other social media provided a springboard to commenting on the situation. Twitter quickly spawned the hashtag, #facebookdown, where tweeters mocked themselves for not knowing what to do without being able to post selfies to Instagram or personal news to Facebook.

"are you kidding me? east bay emergency dispatch says 5 people called 911 during #facebookdown today!" tweeted Kristen Sze (@abc7kritensze). Reports that people were roaming the streets of Berkeley, shoving photos of themselves into strangers’ faces, and asking if they "liked" them, were probably exaggerated.

Mark Your Calendars: The Pirate Bay Returns on February 1st

Torrent downloads fans anxiously waiting for The Pirate Bay service to be resurrected will surely be happy to hear the team behind it has updated the site to add definitive proof that The Pirate Bay is coming back in some form.

After posting a countdown timer on the site in early January alongside a pirate flag, the team a few days ago replaced it with what looked like a functioning website, though users were still unable to access any of their precious downloads.

The team decided once again to change the appearance of the site and posted an image of a Phoenix on Monday, a symbol of rebirth The Pirate Bay used in previous relaunches of the site, as The Guardian reports.

Other visual elements present on the site include the countdown timer on top and an animation showing a battleship traveling towards an island harbor named welcome home. The non-functioning menu is also still present, suggesting the site will soon be back to regular business.

The Pirate Bay was taken offline by Swedish police in early December, and the team behind it having not resumed the site s activity ever since.

Amazon Ramps Up Enterprise Push with Email Service

Amazon.com Inc accelerated its efforts to win over corporate clients on Wednesday by announcing an email and scheduling service that will compete with Microsoft Corp and Google Inc.

The service, dubbed WorkMail, will launch in the second quarter and has been developed by the company's cloud computing unit, Amazon Web Services (AWS). It highlights Amazon's efforts to convince deep-pocketed companies, called enterprises in tech parlance, to shift more of their work to AWS.

Launching an email and scheduling service is likely the first step toward a broader suite of Amazon tools to gain corporate clients, analysts said. For example, Google's Gmail offers many other services beyond email and calendars including file-sharing and video conferencing.

AWS has spent the last couple of years trying to get corporate clients on board because big businesses spend more on data centers than startups, who were the initial focus of its business. But there are concerns that Amazon is spreading itself too thin, given its other sizeable investments in areas like Hollywood-style production and consumer devices.

"Email is a Trojan Horse into the enterprise," Baird analyst Colin Sebastian said. He added that email is a $1 billion opportunity for Amazon given the popularity of AWS and Amazon's willingness to sacrifice margins for volume.

If Amazon adds more services for companies, it could bring in about $10 billion more in extra revenue, Sebastian said.

Microsoft Clarifies How the Spartan Browser Will Support Legacy Sites and Apps

Microsoft answered a few questions about its leading-edge Spartan Web browser on Tuesday.

The new browser, code-named "Project Spartan," is being built for Windows 10, although it isn't part of the latest Windows 10 preview release (build 9926). Spartan will exist alongside IE 11 when the finished Windows 10 product gets released, which is expected to occur sometime in the latter part of this year. A preview of Spartan is expected to arrive in a coming Windows 10 preview release.

Many of Microsoft's answers about Spartan were at the technical level for developers in a Twitter #AskIE thread on Tuesday. However, Jacob Rossi, a senior engineer on the Microsoft Web platform team, provided more general details in a Smashingmagazine.com post this week.

Spartan and Legacy Support?Rossi shed more light on how Microsoft plans to deliver a new Spartan Web browser while also permitting organizations dependent on older Internet Explorer technologies to retain compatibility with their legacy Web apps and intranet sites.

The Spartan browser will have a new rendering engine, called "EdgeHTML," which is the result of Microsoft forking of the Trident engine code used

for Internet Explorer. Spartan will contain both engines, the new EdgeHTML one as well as the legacy Trident engine called "MSHTML".

Organizations will be able to use the Spartan browser even if they have legacy IE support issues to address. When legacy support needs arise, Spartan will be capable of running the old IE Trident engine via Enterprise Mode. Microsoft's Enterprise Mode technology is an IE 11 solution that emulates earlier IE browser technologies all of the way back to IE 5 for compatibility purposes.

"We want enterprises to be able to use Spartan too," Rossi explained. "For them, Trident compatibility (e.g. with legacy line of business sites) is critical. So Spartan can load Trident through Enterprise Mode for those sites. That helps keep their mission critical stuff working while the web gets the latest modern engine, EdgeHTML."

Rossi added that "we will not be getting rid of Trident." It'll be around to support legacy enterprise sites. "This dual-engine approach enables businesses to update to a modern engine for the web while running their mission critical applications designed for IE of old, all within the same browser."

IE also will contain both rendering engines, so the natural question is, Why would Microsoft be planning to sustain two browsers? Why not just stick with Spartan, going forward? Microsoft's engineers did not answer that question directly, although the heavy suggestion in their comments is that Spartan will let Microsoft jettison a lot of old IE code, producing a more lightweight browser. A Microsoft blog post pointed to a blog post by Justin Rogers, a developer on the Spartan project, who highlighted that idea. Rogers suggested that Spartan will allow Microsoft to remove so-called "undead code" that can lead to browser crashes.

Rossi explained that the launch of Spartan will highlight Microsoft's efforts in supporting Web standards. IE tends to remind developers of Microsoft's older and quirky implementations, he added. Spartan does away with the old document-mode support approach in IE, for instance. Spartan also drops support for VBScript, X-UA-Compatible strings, currentStyle and attachEvent legacy coding, he added. Spartan comes with a "new user agent string" that results in "surprisingly positive results in compatibility," according to Rossi. He put in a familiar Microsoft plug that Web site developers should just avoid using user agent sniffing approaches to enable browser compatibility "at all costs." Microsoft's engineering team is aiming to "ensure that developers don't have to deal with cross-browser inconsistencies" with the new Spartan approach, Rossi added.

Developers won't have issues in dealing with two browsers for Windows 10 since Microsoft's next IE version for Windows 10 has "the same dual-engine approach as Spartan," Rossi assured. They both also use Microsoft's Chakra JavaScript engine.

Microsoft is planning to expand standards support with Spartan "in the near future" with support for "Web Audio, Image srcset, @supports, Flexbox updates, Touch Events, ES6 generators, and others," Rossi stated. More distant plans include support for "Web RTC 1.1 (ORTC) and Media Capture (getUserMedia() for webcam/mic access)."

Questions and Answers?Additional Spartan plans were described in Microsoft's Twitter session today. For instance, the dev team confirmed that it plans to add support in Spartan for browser extensions (also

called "plug-ins").

"Yes, we're working on a plan for extensions for a future update to Project Spartan," the team stated.

The team was asked, "What are exactly and precisely the rules to trigger the old IE engine?" It's based on Enterprise Mode in IE ("EMIE"), according to the team.

"Will only honor custom docmodes for intranet sites, sites on Enterprise CV list, and when in EMIE," the team stated. "EdgeHTML will be default for the Internet and X-UA-Compatible will be ignored on internet sites."

The team was asked how frequently Spartan's engine will get updated, answering that the "exact cadence is still TBD, but our intent is to keep regularly updated along with Windows 10 as a whole."

The team was asked if Spartan would be made available for Windows 7. "Spartan is currently targeted at Win10," the team stated. "We're focused on getting ppl [people] upgraded (free) but will watch Win7 demand."

One questioner asked if Spartan would "replace" IE on Windows 10 machines." Consumers on Windows 10 will get Spartan by default," the team stated. "IE will be available for Windows 10 and can be enabled by the user."

6 Ways To Ruin an Email

Continuing with my January series on feigned self-improvement, I dive deeper into the familiar and exhausting practice of email writing, an art and an affliction.

If you are an overworked human like most of us, your inbox is probably an abyss of unanswered messages, relentless promotions, and forwarded chain messages from your Aunt Kathy. In fact, it is probably very rare that you get an email you actually enjoy reading.

Perhaps, you, too, have been the culprit of writing a garbage email. It s not entirely your fault. It may be our general disenchantment with the inbox, but many of us have become mediocre email writers, people we prefer not to be.

We do not expect greatness in our virtual mail bin, and therefore we do not deliver it either.

But your mediocrity ends in 2015. Below are some of the most typical email offenses to avoid. Take notes, people; you ll need them.

As New York Magazine's Science of Us recently observed, the exclamation mark, once reserved for expressing joy or excitement, now simply marks baseline politeness. This is unfortunately true, due to the fact that (as research suggests) it s much harder to convey emotion via text. Still, there s a fine line between showing good intentions and sounding like you re on speed.

As a rule, limit an email to two exclamation points at most. Don t use one after a salutation or a farewell, because that s just unnecessary.

Reserve them for statements that might otherwise be misinterpreted as demanding, cold, or unfeeling (see this for reference). Never use two or more in a row unless you are intentionally mocking your preceding statement.

You might be thinking, what does this girl know about punctuation? Barely anything! But I do spend at least eight hours every day being annoyed by the Internet.

A cruel lingual disease grabs hold after you enter the workforce. Phrases like please advise, going forward, looping in X, or let s circle back on this seep into our lexicon and therefore our emails. They are the bane of the email-buried thought worker s existence, the equivalent of staring at a screen full of 0s and 1s for hours at a time.

This language can be easily avoided and/or made fun of, depending on your superior s sense of humor. Next time you catch yourself writing a phrase that sounds like something out of an episode of The Office, take a moment to translate whatever phrase you were about to write down. Please advise can become What do you think? Looping in X can become I m including X in this conversation, because she d be a helpful person to have on this project.

Mostly, don t abandon your personality for the sake of brevity. Make jokes. Be real. Point out the absurdity of America s standard workplace communication practices. People will answer your emails (and like you more) if they re fun to receive.

There s a reason that old fancy people like Jean-Paul Sartre used to start his letters to Simone de Beauvoir with My dear little girl (aside from being tragically French). It s because those letters took time to arrive. He needed to convey tenderness and longing between postage deliveries.

Now it takes, at most, a few seconds to send an email. Which means it s acceptable to drop some of the typical conventions you might find in an IRL paper letter.

So, if you re reaching out to someone, you should definitely start with Hi X or, if they are a considerable pay grade above you and you ve never come close to an introduction, Dear X. You should also finish off the message with a Thanks, or Best, again depending on your professional distance.

But as soon as the conversation gets going, there s no need to continue with the greetings and farewells. If an adult human is using email to communicate, they will not be offended by your lack of pleasantries in a fast-paced digital conversation. This is a chance for brevity. Take it.

When it comes to signature farewells, please remain conservative. Don t try to be a hero. Sincerely, for instance, is kind of dated. Yours truly, or As ever, are weirdly intimate and trying too hard. Cheers feels imposter-y and British. Best is bland but fine, the equivalent of putting a blank space before a comma. Usually your best bet is Thanks. It s appropriate because you just made a person read an email, and they deserve gratitude for that. It could also be THANKS if someone actually did you a huge favor.

Remember, there is no one right sign-off. Adapt your tone based on the recipient. My goodbyes to BeyoncØ versus, say, Donald Trump, would be

entirely different.

It s wonderful that you ve figured out to permanently stamp every email you write with your name and title. But that does not give you the authority to write a small biography on your life. Please keep the list of accomplishments and social handles short. At most, you should have your name, title, company, two phone numbers, and ONLY one social handle.

Do not include a quote from Gandhi or Mother Teresa or anyone, really. If you email often with a person about mundane things, ultimately the content of your messages will look ridiculous alongside an inspirational quote. Nothing says I m a jerk like a gossipy email about Jill from HR s outfit followed by a quote that says My life is my message.

Fonts have connotations. Like, if I sit down at a restaurant whose menu is written in Comic Sans, I pretty much expect to get food poisoning. The same judgment applies to the words in your emails. Unless you are a graphic designer whose font judgment is sought after, do not stylize the default text on your emails. Or enlarge it. Or make it colorful. Dear God, don t make it colorful.

Follow these easy tips, my dear desk-chained employees, and your digital existence might just get better. If it doesn t, consider more extreme measures.

=~=~=~=